UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/829,761	04/10/2001	Thomas E. Chefalas	YOR920010015US1	9588

35526 7590 10/05/2004

DUKE. W. YEE
YEE & ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
AKPATI, ODAICHE T	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/829,761	**Applicant(s)** CHEFALAS ET AL.	
	Examiner Tracey Akpati	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 August 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☑ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/19/03, 10/21/02*.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-10, 12, 20, 22, 30 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold et al (5440723) in view of Serverwatch—Network Associates Ships CyberCop Sting.

With respect to Claim 1, Arnold et al meets the limitation of "a local server" on Fig. 1A; and "a plurality of client data processing systems" on Fig. 1B; and "...broadcasts an indication that a virus attack is underway to all devices within the network data processing system" on column 2, lines 30-33, column 24, lines 32-42; and "ignores all further access requests by the offending system until receiving an indication that the offending system has been disinfected, and directs the local server to disconnect the offending system from the network data processing system" on column 5, lines 59-65, and on column 24, lines 44-57. Arnold however does not meet the following limitation.

The limitation of "a bait server, wherein the bait server monitors itself and, responsive to an attempt from an offending system within the network data processing system to access the bait server" is met by Serverwatch on pages 1 and 2.

It would have been obvious to combine the teachings of Serverwatch within the system of Arnold et al because the bait server provides a dedicated, convenient and less expensive way of monitoring a large network. A dedicated bait server requires less maintenance than multiple decoy programs/servers and hence simplifies an administrator's job of protecting the network. It is obvious to ignore all further access requests from the offending system until the infected system is uninfected so as not to spread the virus to the rest of the network.

With respect to Claim 2, Arnold et al meets all the limitation except for the following limitation. The limitation of "wherein the address of the bait server is not published to the plurality of client data processing systems" is met by Serverwatch on page 1. This is because the decoy server creates a fictitious presence within the network.

It would have been obvious to combine the teachings of Serverwatch within the system of Arnold et al because the bait server provides a dedicated, convenient and less expensive way of monitoring a large network. A dedicated bait server requires less maintenance than multiple decoy programs/servers and hence simplifies an administrator's job of protecting the network.

With respect to Claim 3, Arnold et al meets the limitation of "wherein the offending system includes more than one data processing system" on Fig. 1C.

With respect to Claim 4, Arnold et al meets the limitation of "wherein the offending system includes the local server" on Fig. 1C.

With respect to Claim 5, Arnold et al meets the limitation of "wherein the offending system includes a client data processing system" on Fig. 1C.

With respect to Claim 6, Arnold et al meets all the limitation except for the following limitation. The limitation of "wherein the attempt from the offending system to access the bait server comprises an attempt to write to the bait server" is met by Serverwatch on page 1. The writing to the bait server is a form of suspicious activity.

It would have been obvious to combine the teachings of Serverwatch within the system of Arnold et al because the bait server provides a dedicated, convenient and less expensive way of monitoring a large network.

A dedicated bait server requires less maintenance than multiple decoy programs/servers and hence simplifies an administrator's job of protecting the network.

With respect to Claim 7, Arnold et al meets the limitation of "wherein the virus is a worm" on column 4, lines 60-66.

With respect to Claim 8, Arnold et al meets the limitation of "wherein the virus is a Trojan horse" on column 4, lines 60-66.

With respect to Claim 9, Arnold et al meets the limitation of "wherein the network data processing system is configured to, once the offending system has been disinfected of the client, allow the offending system to reconnect to the network data processing system" on column 5, lines 59-65 and on column 21, lines 30-42. It is obvious to allow the disinfected system to be reconnected to the network after disinfection.

With respect to Claim 10, Arnold et al meets the limitation of "identifying an offending system from which the request originated" on column 19, lines 46-48; and "alerting a local server that a virus attack is in progress and of the identity of the offending system; and directing the local server to disconnect the offending system from the network" on column 19, lines 60-64 and on column 20, lines 1-3. It is obvious to disconnect the infected computers from the network before the systems are cleaned up so as to prevent further spread of the virus. The "I'm infected" message sent by the infected system(s) inherently has its identifying information as part of the message sent or else the recipient of this message would not know which computer in the network had sent this message. Arnold et al however does not meet the following limitation.

The limitation of "receiving, at a bait server, a request to perform a function on the bait server" is met by Serverwatch on pages 1 and 2.

It would have been obvious to combine the teachings of Serverwatch within the system of Arnold et al because the bait server provides a dedicated, convenient and less expensive way of monitoring a large network. A dedicated bait server requires less maintenance than multiple decoy programs/servers and hence simplifies an administrator's job of protecting the network.

With respect to Claim 12, Arnold et al meets the limitation of "receiving a reconnect request from the offending system; and verifying that the offending system is disinfected and available to reconnect to the network; and reconnecting the offending system to the network" on column 24, lines 61-65. It is inherent that the computer is reconnected to the network after the disinfection is verified.

With respect to Claim 20 and 30, its limitation is similar to Claim 10 limitation and hence its rejection can be found therein.

With respect to Claim 22 and 32, its limitation is similar to Claim 12 limitation and hence its rejection can be found therein.

Claims 11, 21, 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold et al (5440723) in view of Serverwatch—Network Associates Ships CyberCop Sting in further view of Kim et al (6701440 B1).

With respect to Claim 11, all the limitation is met by the combination of Arnold et al and Serverwatch except for the following limitation. The limitation of "prior to disconnecting the offending system, notifying the offending system that it is infected with a virus" is met by Kim et al on column 3, lines 45-47 and 54-61.

It would have been obvious to one of ordinary skill in the art to combine the teachings of Kim et al within the combination of Arnold et al and Serverwatch because quarantining the infected machine and then notifying it that is has been infected prevents further spread of the virus to the rest of the network.

With respect to Claim 21 and 31, its limitation is similar to Claim 11 limitation and hence its rejection can be found therein.

Claims 13, 23, 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Serverwatch—Network Associates Ships CyberCop Sting.

With respect to Claim 13, Serverwatch meets the limitation of "monitoring files within the bait server; and responsive to a change in one or more of the files within the bait server, notifying a local server that a virus attack is underway" on pages 1 and 2. CyberCop notifies an administrator of intrusive activity. This administrator must reside over a server/processor to receive this message.

It would have been obvious to one of ordinary skill in the art to respond to a change in one or more files within the bait server because this would alert the administrator of an ongoing or potential attack within the network.

With respect to Claims 23 and 33, its limitation is similar to Claim 13 limitation and hence its rejection can be found therein.

Claims 14, 15, 24, 25, 34 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Serverwatch—Network Associates Ships CyberCop Sting in view of Arnold et al (5440723).

With respect to Claim 14, Serverwatch meets all the limitation except for the following limitation. Arnold et al meets the limitation of "wherein the change in one or more of the files includes a change in byte size of the one or more of the files" on column 5, lines 14-16.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Arnold et al within the system of Serverwatch because a checksum of the file to indicate that the file has been changed allows the system to know if the server has been infected by a virus.

With respect to Claim 15, Serverwatch meets all the limitation except for the following limitation. Arnold et al meets the limitation of "wherein the change in one or more of the files includes one of a missing and a deleted file." on column 5, lines 14-16.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Arnold et al within the system of Serverwatch because a checksum of the file to indicate that the file has been altered allows the system to know if the server has been infected by a virus.

With respect to Claim 24 and 34, its limitation is similar to Claim 14 limitation and hence its rejection can be found therein.

With respect to Claim 25 and 35, its limitation is similar to Claim 15 limitation and hence its rejection can be found therein.

Claims 16-19, 26-29, 36-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold et al (5440723).

With respect to Claim 16, Arnold et al meets the limitation of "monitoring a network for the presence of a computer virus" on column 2, lines 51-55; and "responsive to a determination that a virus is detected, determining the identity of an offending system within the network from which the virus entered the network" on column 4, lines 61-66; and "directing the local server to disconnect the offending system from the network" on column 19, lines 60-68, and on column 20, lines 1-3.

It would have been obvious to one of ordinary skill in the art at the time of the invention to disconnect the infected computers from the network before the systems are cleaned up so as to prevent further spread of the virus. The "I'm infected" message sent by the infected system(s) has its identifying information as part of the message sent or else the recipient of this message would not know which computer in the network had sent this message and was infected.

With respect to Claim 17, Arnold et al meets the limitation of "instructing all devices within the network to ignore all requests from the offending system until the offending system has been disinfected and is available for network communication" on column 19, lines 60-68 and on column 20, lines 1-11.

With respect to Claim 18, Arnold et al meets the limitation of "notifying a local server of the presence of the virus and the identity of the offending system" on column 19, lines 60-64.

With respect to Claim 19, Arnold et al meets the limitation of "responsive to an indication that the offending system has been disinfected and responsive to a reconnect request from the offending system, reconnecting the offending system to the network" on column 24, lines 61-65.

With respect to Claim 26 and 36, its limitation is similar to Claim 16 limitation and hence its rejection can be found therein.

With respect to Claim 27 and 37, its limitation is similar to Claim 17 limitation and hence its rejection can be found therein.

With respect to Claim 28 and 38, its limitation is similar to Claim 18 limitation and hence its rejection can be found therein.

With respect to Claim 29 and 39, its limitation is similar to Claim 19 limitation and hence its rejection can be found therein.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 703-305-7820. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Please note the Patent Office will be moving to the Alexandria campus next month. The new phone number for myself, Tracey Akpati is (571) 272-3846, my SPE, Kim Vu is (571) 272-3859 and the receptionist is (571) 272-2100.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

OTA